(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020010079162 A
(43)Date of publication of application: 22.08.2001

(21)Application number: 1020010034583
(22)Date of filing: 19.06.2001

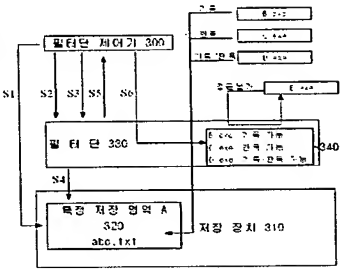
(71)Applicant: TERUTEN
(72)Inventor: KIM, SEONG YEOP
LEE, SAE ROK
LEE, YEONG
YOON, SEOK GU

(51)Int. Cl H04L 9/32

(54) SECURITY SYSTEM FOR SAFE TRANSMISSION AND EXECUTION OF DIGITAL DATA

(57) Abstract:

PURPOSE: A security system is provided to achieve a user convenience and prevent digital content data from being copied, distributed and used by an unauthorized person.



CONSTITUTION: A security system comprises the first storing unit for receiving and storing data; an access control unit for storage of the identification information for the execution program for executing data stored in the first storing unit; a determination unit connected to the access control unit, and which determines whether or not the identification information for the execution program is stored in the access control unit in case where the execution program calls data file; and a transmitting unit connected to the first storing unit and the determination unit, and which transmits data stored in the first storing unit to the execution program, if it is determined by the determination unit that the identification information for the execution program is stored in the access control unit.

Legal Status
Date of final disposal of an application (20021101)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 9/32

(11) 공개번호 특2001-0079162
(43) 공개일자 2001년08월22일

(21) 출원번호 10-2001-0034583
(22) 출원일자 2001년06월19일

(71) 출원인 (주)테르텐
윤석구
서울특별시 강남구 대치동 901-66번지

(72) 발명자 이새록
서울특별시광진구자양3동우성2차아파트202-1208
김성엽
서울특별시광진구군자동372-2
윤석구
경기도안양시동안구범계동목련우성아파트505-1703
이영
경기도안양시동안구범계동목련우성아파트505-1703

심사청구 : 있음

(54) 디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템

요약

본 발명의 목적은 디지털 데이터들의 입출력 및 실행에 있어서, 이를 인증받은 특정 실행 프로그램만이 실시할 수 있도록 하는 디지털 데이터 보호 방법 및 시스템을 제공하는 것이다. 구체적으로 본 발명의 디지털 데이터의 실행 보안 시스템은 디지털 데이터를 입력받아 저장하는 제1 저장 수단과, 상기 디지털 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 저장한 접근 제어 수단과, 상기 접근 제어 수단에 연결되고, 소정의 실행 프로그램이 상기 디지털 데이터 파일을 호출하는 경우에 상기 소정 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 기록되었는지를 판단하는 판단 수단과, 상기 제1 저장 수단 및 판단 수단에 연결되면서, 상기 판단 수단으로부터 상기 실행 프로그램의 식별 정보가 기록되었다는 판단 신호를 입력받으면, 상기 제1 저장 수단으로부터의 상기 디지털 데이터를 상기 소정의 실행 프로그램으로 전송하여 실행토록 하는 전송 수단을 포함한다.

대표도
도 3

명세서

도면의 간단한 설명

도 1은 기존의 디지털 데이터를 무단으로 사용하는 방법을 모식적으로 나타낸 모식도.

도 2는 기존의 DRM 제어기의 실행 방법을 설명하는 모식도.

도 3은 본 발명의 필터단 시스템을 나타내는 모식도.

도 4는 본 발명의 필터단 시스템이 작동하는 방법을 나타내는 모식도.

도 5는 암호화기/복호화기를 포함하는 본 발명의 일 실시예를 나타내는 모식도.

도 6은 실행 가능 프로그램 등록 방법에 관한 본 발명의 또 다른 실시예를 나타내는 모식도.

도 7은 저장 영역을 구분한 본 발명의 또 다른 실시예를 나타내는 모식도.

< 도면의 주요 부분에 대한 설명>

300: 필터단 제어기 330: 필터단

340: 접근 제어 리스트 320: 특정 저장 영역

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 온라인 또는 오프라인으로 제공되는 디지털 데이터를 사용하는 컴퓨터 시스템 및 그 방법과 프로그램 매체에 관한 것으로, 좀 더 상세하게는 소비자가 사용하기 편리하면서도 디지털 데이터를 권한없는 소비자가 무단으로 복제하거나 배포, 또는 사용하는 것을 막는 디지털 데이터 보호 기술에 관한 것이다.

최근 인터넷 등 온라인을 통해 디지털 컨텐츠 데이터의 유통이 일반화되고 있다. 디지털 컨텐츠란 일반적으로 우리가 알고 있는 전통적인 문학 작품, 그림, 영화, 음악 및 게임 등에 더하여 시장 조사 자료, 온라인 교육 내용, 경제적으로 유용한 데이터베이스 등, 시장이나 소비자가 필요로 하는 모든 정보를 포함하는 개념이다.

이러한 디지털 컨텐츠는 대부분 많은 노력을 들여 창조되거나 개발된 것으로, 저작자는 자신의 저작권을 오프 라인과 마찬가지로 온라인 상에서도 보호받고자 하고 있으나, 전통적인 저작권법이나 기타 제도만으로는 온라인이 가지는 무제한의 복제성 및 배포성 때문에 저작권자의 권리를 보호하기에 미흡한 것이 현실이다.

최근 이러한 복제성 및 배포성, 기타 오프 라인상에서 경험하지 못했던 여러 행위를 차단하고, 저작권자의 수익성을 보호하기 위해서, 법률적인 방법에 더하여 기술적인 방법을 사용하여 컨텐츠 이용자의 특정 행위를 제어하는 본격적인 디지털 컨텐츠 보호 기술들이 개발되고 있다. 패스워드 등을 통하여 인증받은 사용자만이 특정 디지털 데이터를 다운로드 받아 사용할 수 있게 한 것이 그 중 하나이다.

최근의 디지털 컨텐츠의 이용은 좀 더 복잡한 보안기술을 요구하고 있다. 즉, 원천적으로 무단 사용을 하는 것이 아니라, 일단 최초 이용은 유료로 다운로드 등을 받아 권한을 가진 사용을 하게 되지만, 이를 하드 디스크 등의 저장 장치에 무단으로 보관한 후, 보관된 파일을 복제하거나 배포하는 2차적 행위에서 저작권자의 권리를 침해하는 양상이 바로 그것이다. 이 경우, 처음의 유효한 사용과 그 이후의 불법적인 사용을 구분해서 제어해야 하는 복잡함이 발생한다.

이러한 문제를 해결하고자 한 방법이 스트리밍 기법인데, 이는 하드 디스크 등의 저장 장치에 데이터를 고정적으로 저장하는 것이 아니라, 데이터의 실시간 다운로드시 프레임별, 또는 데이터 블록별로 컴퓨터 시스템의 램 메모리로 데이터를 저장하여 순간적으로 사용토록 한 다음, 다음 프레임이 다운로드되면 전 프레임의 데이터를 삭제하는 방식이다. 하지만 이것은 통신 속도나 기타 압축 등의 문제로 인하여 동영상의 경우, 화면의 연결이 부드럽지 못하고, 데이터 엉킴(data congestion)이 자주 발생하여 사용자에게 불편을 안겨주는 문제를 안고 있다.

따라서, 데이터 파일 전체를 다운로드 받아서 이를 실행시킬 수 있도록 하면서도 사용자가 무단으로 이를 저장하여 이용하지 못하도록 하는 방법이 절실히 요구되고 있다.

데이터 파일 전체를 암호화해서 배포함으로써 상기와 같은 문제점을 해결하고자 하는 제안이 있었다. 즉, 암호화된 데이터 파일은 인증 받은 키(key)로만 복호화할 수 있으므로, 키를 구비하지 않는 한 데이터 파일 자체로는 실행 프로그램에서 수행되지 않도록 한 것이다. 이 방법은 최근 가장 널리 사용되는 방법 중 하나이다.

하지만 이 방법도 결점을 갖고 있는데, 도 1을 참조하여 그 문제점을 간단히 설명하면, 가장 기본적인 문제는 컨텐츠 데이터를 실행 프로그램(120)에 로드하기 위해서는 암호화된 데이터 파일 전체(100)를 키로 복호화해서 복호화된 컨텐츠(130)를 임시로 저장 장치내에 저장해야 한다는 것이다. 이 때 사용자가 고의로 이 암호화가 풀린 데이터를 복사하거나 외부로 전송하면(140) 이때부터는 상기 암호화가 아무런 기능을 수행하지 못하고 무력화되는 것이다. 이 문제로 인하여 공급자들이나 컨텐츠 제작 측이 소비자를 불신하게 되고, 이에 따라 컨텐츠 데이터 유통이 많은 제한을 받고 있는 것이 현실이다.

최근 관심이 고조되고 있는 디지털 컨텐츠 불법 복제 방지 기술인 DRM(Digital Rights Management)은 이러한 문제를 해결할, 현재로서는 유일한 대안으로 인식되고 있다.

일반적으로 DRM(Digital Right Management)이란 디지털 컨텐츠 사용을 인증받은 사용이나 사용자에게만 한정하기 위한 일련의 하드웨어 및 소프트웨어 서비스와 기술을 말한다. DRM의 주요 테마 및 기술로는 컨텐츠 암호화 기술, 컨텐츠 저작권을 표시하는 워터마킹 기술, 컨텐츠의 사용규칙과 저작권 표시를 위한 사용 정책(Policy) 표현 언어 기술 및 컨텐츠의 사용내역 및 과금 내역정보의 저장과 처리에 관한 기술 등이 있다.

DRM의 이러한 기능 중에서, 특히 컨텐츠 실행 프로그램이 DRM 제어기를 내장한 후, 이 DRM 제어기로만 풀 수 있는 암호화된 컨텐츠 데이터를 배포하여 사용토록 하면 전술한 2차적인 무단 행위를 방지할 수 있게 된다. 도 2를 참조하여 이를 간단히 설명하면, 즉 암호화된 컨텐츠가 실행되기 위해서는 역시 복호화가 반드시 필요하지만, 기존의 방법과는 달리 DRM 제어기(220)가 실행 프로그램 내부(200) 또는 이에 연계하여 존재하므로 복호화된 데이터가 이 영역의 외부로 나가서 저장될 필요없이 바로 그 내부에 함께 존재하는 실행 프로그램(210)으로 전달되어 실행되도록 구성되어 있으므로, 사용자가 이 영역 내부에서만 처리되는 복호화된 컨텐츠에 허가받지 않은 접근 행위를 할 수 없는 것이다. 따라서, 사용자는 무단 복제 및 배포 행위를 할 수 없게 된다.

이 기술의 문제점은 DRM 제어기를 개발하는 개발사에 따라 그 암호화 및 복호화 방법이 수 없이 다양하다는 것이다. 따라서, 하나의 실행 프로그램이 실행해야 할 컨텐츠 데이터도 다양한 DRM에 의해 복호화된 데이터 일 것이므로, 결국 이 실행 프로그램은 이 다양한 DRM 제어기를 모두 내장해야 한다는 문제점이 발생한다. 이것은 현실적으로 불가능한 일이다. 따라서, 이 방법은 임시적인 방법일 뿐 아니라 이 방법 자체가 또 다른 컨텐츠 유통의 장애물로 등장할 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 디지털 데이터의 입출력 및 실행을 안전하게 수행할 수 있도록 하는 디지털 데이터 보호 방법 및 시스템을 제공하는 것이다.

본 발명의 또 다른 목적은 디지털 데이터의 실행에 있어서, 인증받은 특정 실행 프로그램에만 디지털 데이터가 안전하게 전달되어 실시될 수 있도록 하는 디지털 데이터 보호 방법 및 시스템을 제공하는 것이다.

본 발명의 또 다른 목적은 DRM 제어기의 암호화 방법에 상관없이 실행 프로그램이 디지털 데이터 실행을 제어할 수 있도록 하는 파일 시스템 기반의 디지털 컨텐츠 데이터의 유통 보호 시스템을 제공하는 것이다.

본 발명의 또 다른 목적은 사용자에게 편리하면서, 동시에 컨텐츠 권리자에게는 상대적으로 안전한 디지털 컨텐츠 데이터의 유통 시스템을 제공하는 것이다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위한 본 발명의 디지털 데이터의 실행에 관한 보안 시스템은 디지털 데이터를 입력받아 저장하는 제1 저장 수단과, 상기 디지털 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 저장한 접근 제어 수단과, 상기 접근 제어 수단에 연결되고, 소정의 실행 프로그램이 상기 디지털 데이터 파일을 호출하는 경우에 상기 소정 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 기록되었는지를 판단하는 판단 수단과, 상기 제1 저장 수단 및 판단 수단에 연결되면서, 상기 판단 수단으로부터 상기 실행 프로그램의 식별 정보가 기록되었다는 판단 신호를 입력받으면, 상기 제1 저장 수단으로부터의 상기 디지털 데이터를 상기 소정의 실행 프로그램으로 전송하여 실행토록 하는 전송 수단을 포함한다. 또한, 상기 제1 저장 수단의 입력단에 연결되면서, 상기 디지털 데이터를 암호화하여 상기 제1 저장 수단으로 전송하는 암호화 수단을 추가로 포함할 수 있다. 또한, 상기 판단 수단은, 상기 디지털 데이터가 암호화된 상태로 상기 제1 저장 수단에 저장된 경우에 상기 디지털 데이터를 복호화하여 상기 전송 수단으로 전송하는, 제1 복호화 수단을 추가로 포함할 수 있다.

또한, 본 발명의 시스템은 상기 접근 제어 수단에 연결되고, 상기 디지털 데이터에 연관되어 사전에 설정된 소정의 유효 조건을 구비하고, 상기 디지털 데이터의 실행 명령을 입력받으면 상기 실행 명령이 상기 유효 조건을 만족시키는지를 판단하고, 상기 실행 명령이 유효한 실행 명령이라고 판단된 경우에만 상기 디지털 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 상기 접근 제어 수단으로 전송하여 저장토록 하는 유효 조건 판단 수단을 추가로 포함한다. 상기 디지털 데이터의 암호화는 1회용 키를 이용하여 암호화할 수 있다. 한마디로, 본 발명의 디지털 데이터의 실행 보안 시스템은, 디지털 데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하기 위해 상기 특정 실행 프로그램의 식별 정보를 구비하면서, 임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에 상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하여 상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 디지털 데이터가 실행되도록 하는 필터링 수단을 포함하는 것이다.

또한, 본 발명은 디지털 데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하는 방법에 관한 것으로서, 이것은 디지털 데이터를 저장하는 단계와, 상기 특정 실행 프로그램의 식별 정보를 구비하는 단계와, 임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에, 상기 임의의 실행 프로그램의 식별 정보를 구비하는 단계와, 상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하는 단계와, 상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 디지털 데이터가 실행되도록 하는 필터링하는 단계를 포함한다.

이하, 도면을 참조하여 본 발명의 예시적 실시예를 상세히 설명한다.

도 3은 본 발명의 필터 시스템이 구현된 클라이언트 시스템의 개략적인 블록도이다.

도 3의 필터 시스템은, 클라이언트 시스템의 저장 장치에 특정 영역을 생성하고 특정 실행 프로그램만이 상기 특정 영역에 접근할 수 있도록 필터단을 제어하는 필터단 제어기와, 상기 특정 영역내의 모든 데이터의 입출력을 제어하면서 등록된 특정 실행 프로그램의 데이터 호출만을 유효한 것으로 판정하여 실행토록 하는 필터단으로 구성되어 있다.

그 작동 방식을 상세히 설명하면, 우선 필터단 제어기(300)는 클라이언트 시스템의 저장 장치(310)내에 특정 영역(320)을 구분하여 생성하도록 명령하고(S1), 이 특정 영역을 식별시키는 식별 정보를 필터단에 통보한다(S2). 이 특정 저장 영역 생성은 필터단 제어기(300)가 전술한 것처럼 직접 수행하거나, 또는 필터단(330)에 생성 명령을 내려(S3) 필터단이 특정 영역을 생성하고(S4) 필터단(330)이 생성한 특정 영역에 대한 정보를 필터단 제어기에 보고하는(S5) 간접적인 방법을 취할 수도 있다.

그 다음, 필터단 제어기(300)는 선정된 특정 실행 프로그램의 식별자를 상기 필터단에 통보하여 필터단(330)에 이를 등록하도록 한다(S6). 이 등록된 데이터(340)는 일종의 접근 제어 리스트 역할을 수행하는데, 이 리스트에 의해 상기 특정 영역내의 데이터를 호출하여 실행할 수 있는 실행 프로그램이 결정된다.

도 3에서는 예시적으로 B.exe가 특정 저장 영역 A(320)의 기록 가능 실행 프로그램으로, C.exe가 판독 가능 프로그램으로, D.exe가 기록/판독 가능 프로그램으로 등록된 경우를 보여주고 있다. 또한, E.exe는 필터단에 등록되지 않은 실행 프로그램이다. 이 경우, 가령 저장 영역 A(320)에 abc.txt라는 데이터 파일이 저장되어 있으면, 이 데이터 파일은 상기 B.exe 나 D.exe 만이 저장할 수 있었던 파일이 되며, 상기 C.exe 와 상기 D.exe 만이 호출하여 판독할 수 있을 뿐이다. 따라서 권한을 부여받지 못한 실행 프로그램은 이 데이터를 판독하거나 저장하지 못한다. 상기 E.exe는 판독 및 기록을 전혀 수행할 권한이 없는 프로그램으로 데이터에 대한 접근 자체가 거부된다.

본 발명의 이러한 특징은 기존의 디지털 컨텐츠 보호 방법이나 DRM 제어기가 갖는 문제점을 해결하는 강력한 수단이 된다. 즉, 기존 시스템은 실행 프로그램에 의해 실행되기 직전에 잠시라도 암호화가 풀린 상태로 메모리에 저장되는 컨텐츠 데이터를 사용자가 고의로 유출하거나 저장하는 것을 방지할 방법이 없었다. 또한, 이것을 방지하기 위해서 DRM 제어기와 실행 프로그램이 서로 내장되어 사용되는 방식에서는, DRM 제어기와 실행 프로그램을 서로 짝을 지어 있어야 하는 형태인데, 양자 모두 종류의 다양함으로 인해서 수 많은 짝들이 구비되어야 하는 문제점이 있었다는 것은 전술한 바이다. 이러한 문제점을 한번에 해결한 것이 본 발명의 시스템이다. 왜냐하면, 본 발명을 이용하면, 실행 직전에 암호화가 풀린 컨텐츠 데이터를 호출하여 저장하거나 무단으로 배포할 수가 없기 때문이다. 즉, 등록된 실행 프로그램이나 실행 프로그램만이 컨텐츠 데이터에 접근할 수 있으므로, 이 등록된 실행 프로그램이 저장이나 배포 기능을 수행할 수 없는 것이나 또는 그렇게 되도록 조치를 해 두면, 소비자나 최종 사용자는 그 실행 프로그램으로는 컨텐츠의 실행 외에는 어떠한 행위도 수행할 수 없게 된다. 가령, 도 3에서 판독만이 가능한 실행 프로그램 C.exe만이 등록되어 있다면, 소비자의 무단 행위는 원천적으로 방지된다. 어떠한 실행 프로그램을 등록시킬 것인가에 관한 여부 또한 본 발명의 필터단 제어기가 결정하므로 사용자가 임의로 조작할 수 없는 것이다.

또한, 도 3의 구성은 특정 DRM 제어기에 포함되는 것이 아니다. 따라서, 기존 DRM 제어기가 가진 전술한 문제점인 실행 프로그램이 모든 DRM 제어기를 내장해야 하는 문제점도 발생하지 않게 된다.

이하에서는 본 발명의 이러한 특징을 기존 DRM 제어기와 연계하여 실시하는 한 실시예를 설명토록 한다. 본 발명에서 DRM 제어기는 클라이언트 시스템으로 입력된 컨텐츠를 DRM 제어기가 속한 도메인이 가지는 고유의 암호화 상태로 만드는 기능을 수행하거나, 다운로드 받은 컨텐츠의 확장자나 기타 해당 컨텐츠 데이터에 부가되어 전송된 컨텐츠 이용 정보, 또는 사용 정책(Usage Policy)이 있으면 이를 바탕으로 대응하는 실행 프로그램를 실행시키도록 윈도우 시스템에 명령을 내린다. 또한, 해당 실행 프로그램에 대해 부여된 식별자를 제공받아 하부의 파일 시스템 필터단으로 전달하는 역할을 수행한다.

하지만, 반드시 DRM 제어기가 전술한 기능들을 수행할 필요는 없고, 윈도우 시스템 자체의 모듈이나 기타 방법으로도 수행 가능하다. 따라서 설명되는 실시예는 단지 본 발명의 이해를 돕기 위해 사용한 것일 뿐이며, 본 발명이 반드시 DRM 제어기와 같이 사용될 필요가 없다는 것은 당업자라면 당연히 알 수 있을 것이다.

본 발명에서 실행 프로그램 식별자(identification information, fingerprint)란, 운영 프로그램에서 제공하는 식별자만을 의미하는 것은 아니며, 특정 실행 프로그램의 인증서나 실행 이미지 등도 이에 해당될 수 있다. 간단히 말하면, 실행 프로그램 식별자란 어떤 응용 프로그램이나 실행 프로그램을 다른 어플리케이션과 구분할 수 있는 모든 정보를 포함하는 개념이다. 또한, 본 발명에서 실행 프로그램라고 지칭되는 것은 컨텐츠 데이터 파일을 실행시킬 수 있는 모든 실행 프로그램을 포함하는 개념임을 주목해야 한다.

컨텐츠 데이터와 함께 전송된 컨텐츠 사용 정책 데이터는 이 컨텐츠를 유효하게 사용할 수 있는 모든 정보를 포함한다. 사용자가 컨텐츠 공급자와 맺은 계약에 의해 이용 정보가 결정될 수 있는데, 가령 해당 컨텐츠를 3회만 이용할 수 있다거나, 해당 컨테츠를 다운로드 받은 날로부터 1주일간만 실시할 수 있다거나 하는 것이다. 사용 정책 데이터는 컨텐츠 데이터와 함께 다운로드 될 수도 있고, 혹은 컨텐츠 공급자 측의 서버등에서 수시로 다운로드받아 갱신할 수도 있다.

도 4는 본 발명의 필터단 시스템을 일반적인 DRM 제어기에 응용한 경우를 보여주고 있다. 도 4에서, 클라이언트 시스템에서 요청된 컨텐츠 데이터 abc.txt는 인터넷 등의 네트워크나 또는 CD-ROM 등의 저장 매체를 통해 클라이언트 시스템의 입력 장치(460)로 입력되고(S2), 이 컨텐츠 데이터는 DRM 제어기(440)에 의해서 DRM 제어기가 속한 도메인이 가지는 고유의 암호화 방법으로 암호화되어 클라이언트 시스템의 저장 장치(450)에 저장된다(S3). 이 데이터는 향후 DRM 제어기에 의해 다시 복호화되는데, DRM 제어기의 암호화 및 복호화 방법은 DRM 제어기 공급 업체마다 다르며 당업자에게 잘 알려진 기술이다.

한편, 본 발명의 필터단 제어기(400)는 사전에, 또는 자신의 실행때마다 저장 장치(410)내에 특정 저장 영역 A(420)를 생성해 둔다.

상기 저장된 컨텐츠 데이터 abc.txt 를 특정 실행 프로그램 프로그램 B.exe에서 실행하기 위해서는, 소비자가 자신의 클라이언트 시스템에서 탐색기나 기타 방법을 통해 해당 컨텐츠를 선택해야 한다. 컨텐츠를 선택했다는 신호가 DRM 제어기(440)로 입력되면, DRM 제어기는 우선, 자신이 가지고 있거나 또는 원거리 서버로부터 전송받을 수 있는 사용 정책 데이터를 체크하여 이 선택 및 실행이 유효한 것인지를 판단한다.

전술한 바와 같이, 이 사용 정책은 해당 컨텐츠를 유효하게 이용할 수 있는지를 체크하는 것으로서, 가령 3회 이용 제한이 된 컨텐츠인 경우, 지금까지의 사용 횟수가 저장되어 있으므로 내장된 카운터 및 비교기를 이용하여 그 유효성을 검사하는 것이 하나의 예가 될 수 있다. 이용 일수가 제한된 경우에는, 시스템 클록(clock)을 이용하여 그 유효성을 검사할 수도 있다. 이러한 경우들은 클라이언트 시스템 내에서만 이루어지는 체크이므로 특별히 이를 로컬 인증이라 할 수 있다. 로컬 인증 외에 또 다른 인증 방법으로는, 실행 명령을 인식한 DRM 제어기가 자동적으로 컨텐츠 공급자 측의 인증 서버(도시되지 않음)에 연결하여, 그로부터 유효성 검사를 체크받고, 인증을 얻을 수도 있다. 이 경우는 DRM 제어기가 사용 정책을 갖지 않고 처음부터 서버로부터 인증을 받도록 계획된 것이다. 이를 본원 발명에서는 원거리 인증이라 한다. 물론, 상기 로컬 인증의 경우에도 사용 정책이 갱신된 경우, 가령 사용 계약의 갱신 등에 의해 컨텐츠 사용 횟수 등에 변경이 있으면 서버에 연결하여 새로운 사용 정책을 다운로드 받아 사용할 수도 있다.

소비자의 사용 명령이 유효한 것이라고 판단되면, 저장 장치(450)에 저장된 컨텐츠 데이터는 호출되어(S4) DRM 제어기(440)에 의해 복호화된 다음, 필터단(430)을 거쳐 저장 영역 A(420)에 저장된다(S5).

또한, 필터단 제어기(400)는 DRM 제어기(440)으로부터 컨텐츠 데이터 abc.txt를 사용할 것이라는 통보를 받으면(S6) 파일 시스템 필터단(430)에 이 컨텐츠 데이터를 실행할 수 있는 실행 프로그램, 또는 실행 프로그램인 B.exe의 식별자 등을 내부의 리스트(470)에 등록한다(S7).

하부의 파일 시스템 필터단(430)은 저장 영역 A(420)에 대한 모든 데이터 입출력을 통제하고 있는 모듈이다. 여기서 파일 시스템이란 특정 저장 영역과 실행 프로그램 간의 인터페이스를 지칭하는 것으로서, 모든 파일 관련 시스템 호출을 필터링하여 등록되지 않은 실행 프로그램의 컨텐츠 파일 접근을 통제한다. 또한, 실행 프로그램과 필터단 사이에서는 암호가 풀린 상태로 데이터가 전송되므로, 이 사이에는 아무런 다른 침입이 없어야 한다. 따라서 암호가 풀린 데이터를 전송하는 필터단 내부의 모듈로부터 인증받은 실행 프로그램간에 어떤 임의의 모듈이나 파일, 또는 명령이 끼어 들어 자신의 행동을 방해하지 않도록, 파일 시스템 필터단은 항상 통신 경로를 체크하고 모듈이나 파일이 있으면, 실행 프로그램 방향으로 자신을 전진 위치시켜 통신 경로를 클리어링하는 기능도 동시에 수행한다. 또한, 침입이 발견되었을 때, 오류를 보고하거나 침입을 자동으로 제거하는 기능도 동시에 수행할 수 있다.

전술한 기능들은 일반적으로 필터단 내부의 펑션 포인터(function pointer)를 이용하여 구현할 수 있다. 필터단을 시스템에 등록할 때 바로 이전 필터단이 있을 경우, 시스템은 이 이전 필터단의 어드레스를 새로 등록되는 필터단에 제공하게 된다. 이러한 필터단의 성질을 이용하면 되는데, 가령 본 발명의 필터단의 전단에 알 수 없는 필터단이 임의로 침입한 경우를 대비해서 주기적으로, 또는 실행 프로그램에 암호화가 풀린 데이터를 전송하기 직전에, 본 발명 필터단의 실행 프로그램 방향으로의 전단에 테스트 필터단을 등록시키고, 이 테스트 필터단에 제공되는 어드레스를 체크한다. 이 어드레스가 본 발명의 필터단이라면 본 발명 필터단의 실행 프로그램 방향으로의 전방에는 테스트 필터단밖에 없지만, 이 어드레스가 다른 것이라면(이 경우 침입 필터단의 어드레스가 되는데) 침입 필터단이 존재하는 것을 의미한다. 이 경우, 본 발명의 필터단을 시스템에서 등록 해지하고, 다시 등록을 하면 본 발명의 필터단이 실행 프로그램 방향으로 최전방에 위치하게 된다.

또는, 상기 테스트 필터단에서 본 발명 필터단으로 직접 호출하도록 코딩하면 된다. 이 외에도 다양한 방법이 사용될 수 있다. 이러한 기능을 수행하는 이유는 본 발명의 파일 시스템 필터단(430)이 저장 영역 A(420)에 대한 모든 데이터 입출력을 자신이 의도하는대로 제어하기 위해서이다.

이 후, 컨텐츠 데이터 abc.txt에 대한 특정 실행 프로그램, 가령 B.exe의 실행 호출이 있으면(S8), 이것은 반드시 파일 시스템 필터단(430)을 거치게 된다. 이 경우, 파일 시스템 필터단은 B.exe가 필터단 제어기에 의해 등록된 실행 프로그램인지를 체크하고 이것이 등록된 실행 프로그램임을 내부 등록 리스트(470)를 통해 인지하면, 이 호출에 대한 응답으로 abc.txt를 B.exe가 실시할 수 있도록 저장 영역 A에서 호출하여 로딩시키다(S9).

반대로 등록되지 않은 C.exe가 상기 abc.txt를 호출하면 파일 시스템 필터단(430)은 이것을 리스트(470)에서 발견하지 못하게 되고, 이 호출에 대해서는 에러 메시지를 통지하거나 또는 무단 사용임을 통지하고 프로세스를 종료한다(S10). 특정 DRM 제어기와는 별개로 작동하면서, 동시에 암호가 풀린 상태로 저장된 컨텐츠 데이터를 무단으로 사용하기 위한 접근을 제어하는 본 발명의 기능을 주목하기 바란다.

도 5는 본 발명 시스템의 또 다른 실시예를 나타내고 있다.

도 5에서 도 4와 동일한 도면 번호는 동일한 기능을 수행하므로 여기서 그 기능들에 대해 다시 설명하지는 않는다. 도 5가 도 4와 다른 점은 암호화기/복호화기(500)를 추가로 구비한다는 것이다. 즉, 컨텐츠 데이터를 파일 시스템 필터단(430) 하부의 저장 영역 A(420)에 저장할 때는 암호화해서 저장하고(S11), 유효한 실행 프로그램이 호출하여 실행해야 할 때는 이를 다시 복호화하여 전달한다(S12). 또한 이 암호화를 풀 수 있는 키 등은 반드시 본 발명의 파일 시스템 필터단(430) 내부에 둔다.

이렇게 컨텐츠 데이터를 암호화하여 저장하고 이 키를 파일 시스템 필터단에 저장하는 이유는, 인증받지 않은 실행 명령을 내리고자 하는 사용자가 임의로 파일 시스템 필터단을 제거하여 본 발명 시스템을 무력화시키는 것을 방지하기 위한 것이다. 즉, 파일 시스템 필터단(420)을 제거하면 이에 저장된 복호화용 키도 제거되므로, 필터단 제거에 의해 저장 영역 A를 사용자가 무단으로 접근할 수 있다 하더라도 내부에 저장된 암호화된 데이터를 풀 수 없게 하고자 하는 것이다.

이 때 암호화는 당업자들에게 잘 알려진 1회용 암호키 기술 등이 이에 사용될 수 있는데, 1회용 암호화는 매번 암호화 및 복호화 키가 변하므로 사용자가 종전 사용 이력으로는 알아낼 수 없기 때문이다. 단계(S12)를 거치는 동안을 전후하여 암호화기/복호화기는 후속 사용을 대비하여 abc.txt를 다시 암호화해서 저장한다.

도 6은 본 발명의 또 다른 실시예를 나타내고 있다. 역시 도 4와 동일한 기능을 수행하는 부분들에 대해서는 동일한 부호를 붙였으며 설명을 생략한다. 도 6은 컨텐츠 데이터와 이를 실행할 수 있는 실행 프로그램을 접근 제어 리스트(470)에 등록하는 방법에 특징이 있다. 가령, 저장 영역 A에서도 컨텐츠 데이터별로 실행 가능한 프로그램을 매칭시켜 상기 리스트(470)에 등록시킨 것이다. 도 6에서는 abc.txt 파일은 B.exe가 실행할 수 있고, efg.txt 파일은 C.exe가 수행할 수 있도록 하였다(S13). 따라서 이 경우에는 컨텐츠 데이터 파일별로 별도의 사용 정책을 가진 경우에 유용한 구성이라 할 수 있다.

도 7은 본 발명의 또 다른 실시예를 나타내고 있다. 역시 도 4와 동일한 기능을 수행하는 부분들에 대해서는 동일한 부호를 붙였으며 설명을 생략한다.

도 7에서는 두 개의 저장 영역(A, B)를 분리하여 설치하고, 파일 시스템 필터단(430)의 접근 제어 리스트(470)에는 각각의 저장 영역에 접근 가능한 실행 프로그램을 별개로 등록한 형태이다. 이 경우는 사용 정책이 다른 컨텐츠 데이터들을 사용 정책별로 분리된 저장 영역에 대응하도록 별개로 저장하여 사용할 수 있도록 하여 사용정책에 따른 컨텐츠 데이터 이용을 좀 더 효율적이 되도록 하였다. 이 경우, C.exe는 저장 영역 B(490)의 데이터만 실행할 수 있을 뿐이다(S14).

발명의 효과

본 발명에서 상기 파일 시스템 필터단 및 접근 제어 리스트의 사용의 장점은 인증되지 않은 사용에서 좀 더 명확해진다.

사용자가 상기 컨텐츠 데이터를 실행시켜 이를 이용할 때, 해당 컨텐츠 데이터는 암호가 풀린 상태로 실행되게 된다. 이 경우, 사용자는 암호가 풀린 이 데이터를 자신의 저장 장치 등에 무단으로 저장하거나 또는 네트워크 상에서 전송할 수 있다.

본 발명의 시스템을 이용하면 이런 문제를 방지할 수 있다. 즉, 암호가 풀린 데이터는 파일 시스템 필터단을 거쳐 오직 인증받은 실행 프로그램에만 제공된다. 또한, 필터단 제어기는 저장 기능이나 자체 전송 기능이 없는 실행 프로그램을 선택하여 실행시키거나, 또는 실행 프로그램의 저장 기능 및 전송 기능을 한시적으로 무력화시킨 상태로 실행되도록 제어할 수 있다. 이는 구체적으로 실행 프로그램의 실행 명령 중, 이러한 명령이 저장 장치의 드라이브나 전송 장치 드라이브로 전달되지 않도록 조치함으로써 구현될 수도 있다.

인증 받지 않은 실행 프로그램으로는 사용자가 상기 컨텐츠 데이터를 실행하는 명령을 내리더라도 파일 시스템 필터단에서 접근 제어 리스트를 통해 이를 무효한 명령으로 판단한 다음, 이를 실행하지 않게 된다. 따라서 사용자는 암호가 풀린 컨텐츠 데이터에도 등록받지 않은 실행 프로그램으로는 접근할 수 없게 된다.

따라서, 기존 시스템에서는 일단 컨텐츠 데이터가 이용자 영역으로 넘어가면, 공급자 입장에서는 막을 수 없었던 저작권 침해 행위가 가능했지만, 본 발명을 이용하면 이를 제어할 수 있게 된다.

본 발명은 컴퓨터 프로그램으로 제작될 수 있고, 또한 제작된 컴퓨터 프로그램은 기록 매체에 저장되거나, 전송 매체에 의해 전송될 수 있다.

본 발명은 특정 운영체제에 국한되는 것은 아니며, 윈도우의 다른 버젼, 유닉스나 기타 체제에서도 동일한 기술적 사상 내에서 당업자라면 다양한 변형을 손쉽게 생각해 낼 수 있을 것이다.

본 발명의 또다른 주요한 효과는 특정 데이터에 대해서 실행 프로그램별 접근 제어를 가능하게 해 준다는 것이다. 기존의 데이터별 또는 사용자별 접근제어는 사용자가 실행 프로그램의 변조등을 통한 권한 확대, 예를 들면 기존의 자신이 갖고 있는 읽기 권한에 더하여 쓰기 권한까지 확대하는것 등을 막을 수 없었다. 본 발명에서는 실행 프로그램을 인식하고, 실행 프로그램에 따라서 접근 제어를 시행하기 때문에 이러한 문제점들을 근본적으로 막을 수 있는 효과가 있다.

본 발명의 필터링 시스템은 일반적인 모든 실행 프로그램과 데이터간에 적용되는 것이며, 특정 컨텐츠 데이터에만 국한되는 것은 아니다.

(57) 청구의 범위

청구항 1.

데이터의 실행에 관한 보안 시스템에 있어서,

데이터를 입력받아 저장하는 제1 저장 수단과,

상기 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 저장한 접근 제어 수단과,

상기 접근 제어 수단에 연결되고, 소정의 실행 프로그램이 상기 데이터 파일을 호출하는 경우에 상기 소정 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 기록되었는지를 판단하는 판단 수단과,

상기 제1 저장 수단 및 판단 수단에 연결되면서, 상기 판단 수단으로부터 상기 실행 프로그램의 식별 정보가 기록되었다는 판단 신호를 입력받으면, 상기 제1 저장 수단으로부터의 상기 데이터를 상기 소정의 실행 프로그램으로 전송하여 실행토록 하는 전송 수단을

포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 2.

제1항에 있어서, 상기 제1 저장 수단의 입력단에 연결되면서, 상기 데이터를 암호화하여 상기 제1 저장 수단으로 전송하는 암호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 3.

제1항에 있어서, 상기 판단 수단은, 상기 데이터가 암호화된 상태로 상기 제1 저장 수단에 저장된 경우에 상기 데이터를 복호화하여 상기 전송 수단으로 전송하는, 제1 복호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 4.

제1항 및 제3항 중 어느 한 항에 있어서, 암호화된 데이터를 저장하고 있는 제2 저장 수단과, 이 제2 저장 수단 및 상기 제1 저장 수단 사이에 연결되면서, 상기 제2 저장 수단에 저장된 암호화된 데이터를 복호화하여 상기 제1 저장 수단으로 전송하는 제2 복호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 5.

제2항에 있어서, 암호화된 데이터를 저장하고 있는 제2 저장 수단과, 이 제2 저장 수단 및 상기 암호화 수단 사이에 연결되면서, 상기 제2 저장 수단에 저장된 암호화된 데이터를 복호화하여 상기 암호화 수단으로 전송하는 제2 복호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 6.

제1항에 있어서, 상기 접근 제어 수단에 연결되고, 상기 데이터에 연관되어 사전에 설정된 소정의 유효 조건을 구비하고, 상기 데이터의 실행 명령을 입력받으면 상기 실행 명령이 상기 유효 조건을 만족시키는지를 판단하고, 상기 실행 명령이 유효한 실행 명령이라고 판단된 경우에만 상기 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 상기 접근 제어 수단으로 전송하여 저장토록 하는 유효 조건 판단 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 7.

제2항 및 제3항 중 어느 한 항에 있어서, 상기 데이터의 암호화는 1회용 키를 이용하여 암호화하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 8.

데이터의 실행 보안 시스템에 있어서,

데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하기 위해 상기 특정 실행 프로그램의 식별 정보를 구비하면서, 임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에 상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하여 상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 데이터가 실행되도록 하는 필터링 수단을 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 9.

제8항에 있어서, 상기 필터링 수단에 연결되면서, 상기 데이터를 저장하는 저장 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 10.

제9항에 있어서, 상기 필터링 수단은, 상기 데이터가 암호화되어 상기 저장 수단에 저장된 경우에 이를 복호화하는 복호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 11.

제9항에 있어서, 상기 필터링 수단은, 상기 데이터를 저장할 때는 이를 암호화하여 상기 저장 수단에 전송하고 상기 저장 장치로부터 상기 데이터를 판독할 때는 상기 데이터를 복호화하는 암호화 수단을 추가로 포함하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 12.

제1항에 있어서, 상기 전송 수단은 상기 소정의 실행 프로그램 방향으로 최전단에 위치하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 13.

제8항에 있어서, 상기 필터링 수단은 상기 소정의 실행 프로그램 방향으로 최전단에 위치하는 것을 특징으로 하는 데이터 보안 시스템.

청구항 14.

데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하는 방법에 있어서,

상기 데이터를 저장하는 단계와,

상기 특정 실행 프로그램의 식별 정보를 구비하는 단계와,

임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에, 상기 임의의 실행 프로그램의 식별 정보를 구비하는 단계와,

상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하는 단계와,

상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 데이터가 실행되도록 하는 필터링하는 단계

를 포함하는 것을 특징으로 하는 데이터 실행 방법.

청구항 15.

제14항에 있어서, 상기 데이터를 저장하는 단계는 상기 데이터를 암호화하여 저장하는 단계인 것을 특징으로 하는 데이터 실행 방법.

청구항 16.

제15항에 있어서, 상기 암호화된 데이터를 복호화하는 단계를 추가로 포함하는 것을 특징으로 하는 데이터 실행 방법.

청구항 17.

제16항에 있어서, 상기 복호화 단계는 상기 필터링 단계가 수행될 때 수행되는 것을 특징으로 하는 데이터 실행 방법.

청구항 18.

컴퓨터 프로그램 전송 매체에 있어서,

데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하기 위해 상기 특정 실행 프로그램의 식별 정보를 구비하면서, 임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에 상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하여 상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 데이터가 실행되도록 하는 필터링 수단을 포함하는 것을 특징으로 하는 컴퓨터로 판독 가능한 프로그램을 전송하는 프로그램 전송 매체.

청구항 19.

제18항에 있어서, 상기 필터링 수단은, 상기 데이터를 저장할 때는 이를 암호화하고 암호화된 상기 데이터를 판독할 때는 이를 복호화하는 암호화 수단을 그 내부에 포함하는 것을 특징으로 하는 컴퓨터로 판독 가능한 프로그램을 전송하는 프로그램 전송 매체.

청구항 20.

컴퓨터 프로그램 저장 매체에 있어서,

데이터의 실행을 특정한 실행 프로그램만이 실행가능토록 하기 위해 상기 특정 실행 프로그램의 식별 정보를 구비하면서, 임의의 실행 프로그램이 상기 컨텐츠를 실행하기 위해 호출할 경우에 상기 구비된 특정 실행 프로그램의 식별 정보와 상기 임의의 실행 프로그램의 식별 정보를 비교하여 상기 두 식별 정보가 일치할 경우에만 상기 호출에 대해 상기 데이터가 실행되도록 하는 필터링 수단을 포함하는 것을 특징으로 하는 컴퓨터로 판독 가능한 프로그램을 기록한 프로그램 기록 매체.

청구항 21.

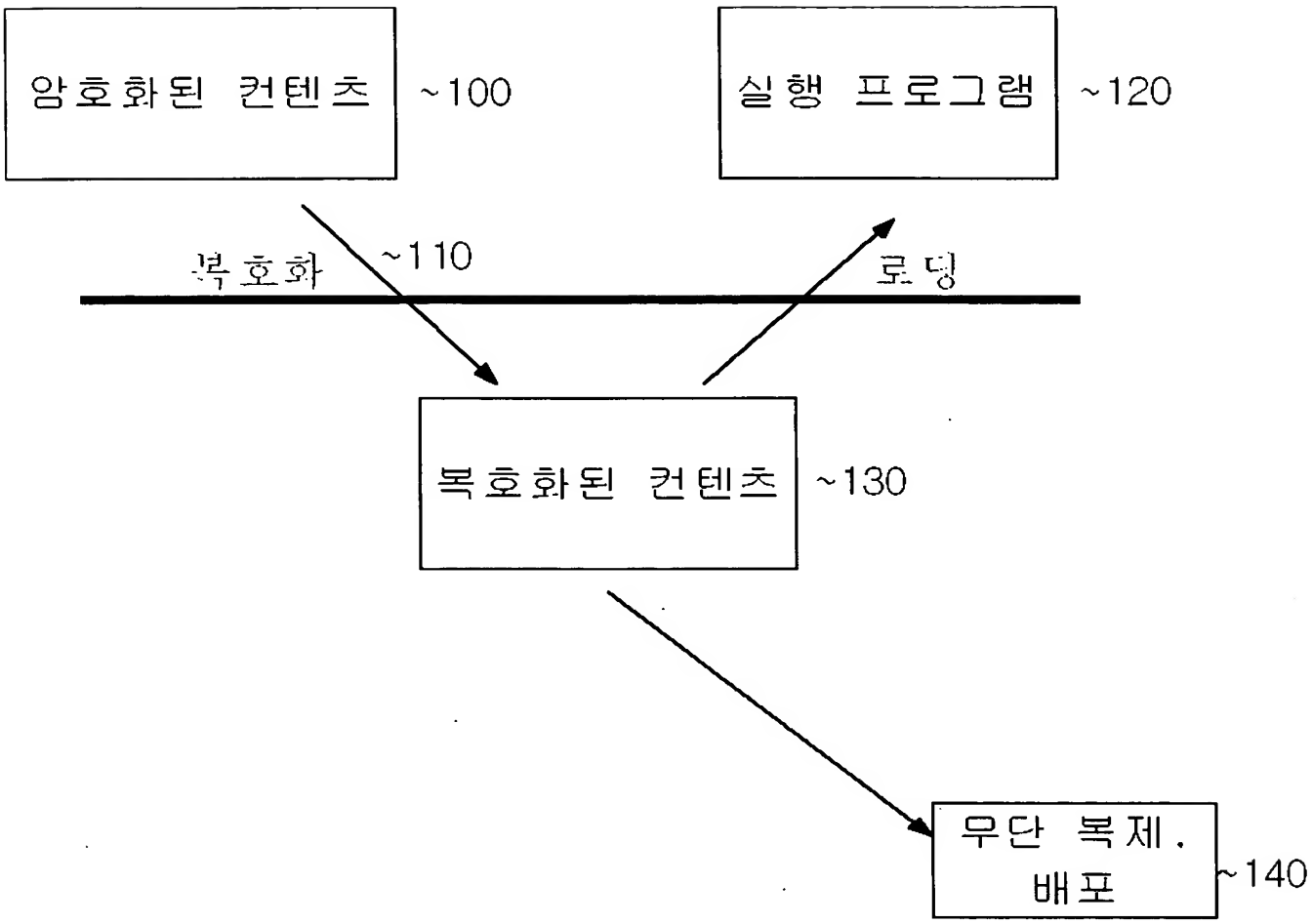
제20항에 있어서, 상기 필터링 모듈은, 상기 데이터를 저장할 때는 이를 암호화하고 암호화된 상기 데이터를 판독할 때는 이를 복호화하는 암호화 수단을 그 내부에 포함하는 것을 특징으로 하는 컴퓨터로 판독 가능한 프로그램을 기록한 프로그램 기록 매체.

청구항 22.

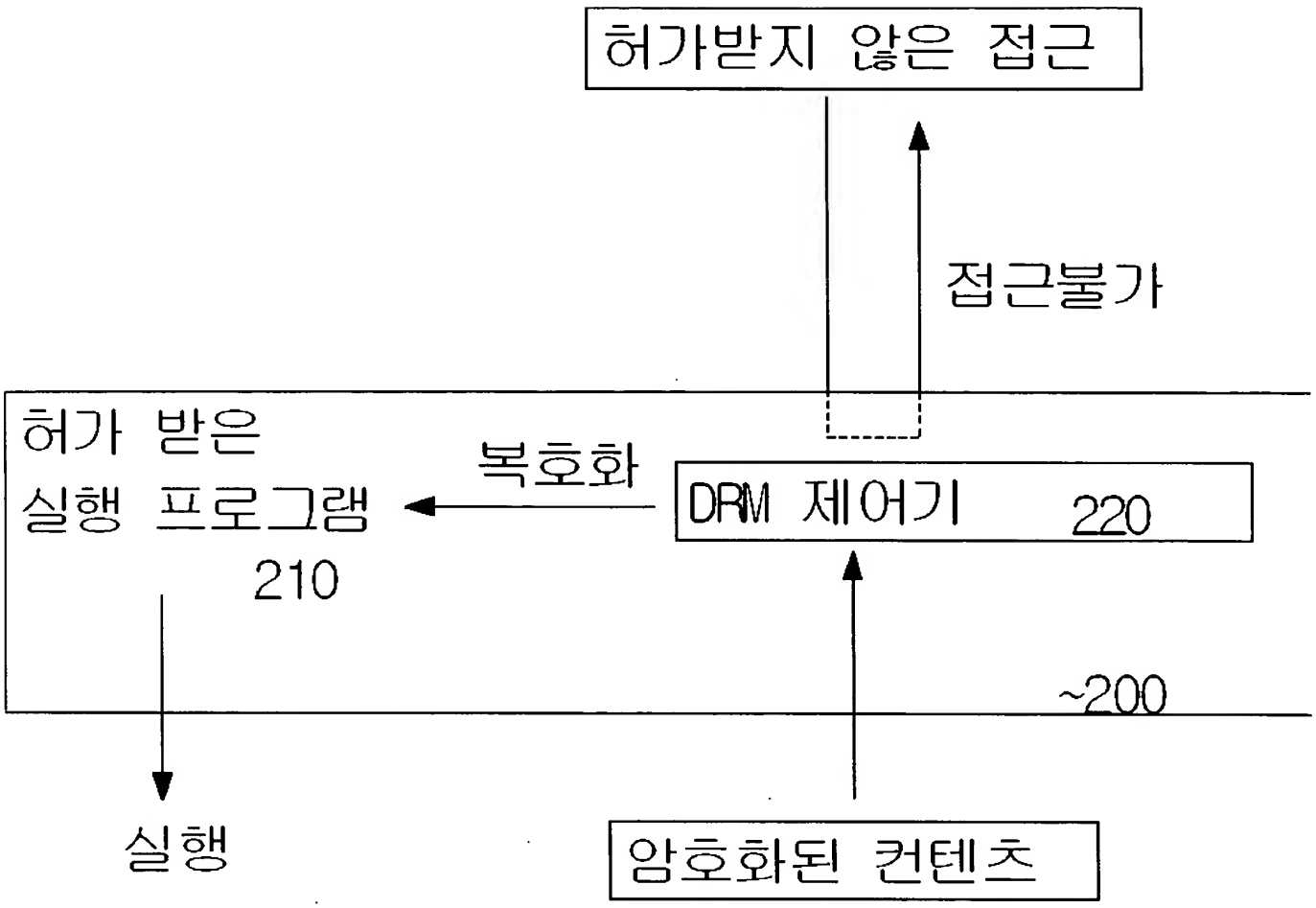
제1항 내지 제7항 중 어느 한 항에 있어서, 상기 데이터는 디지털 컨텐츠 데이터인 것을 특징으로 하는 데이터 보안 시스템.

도면

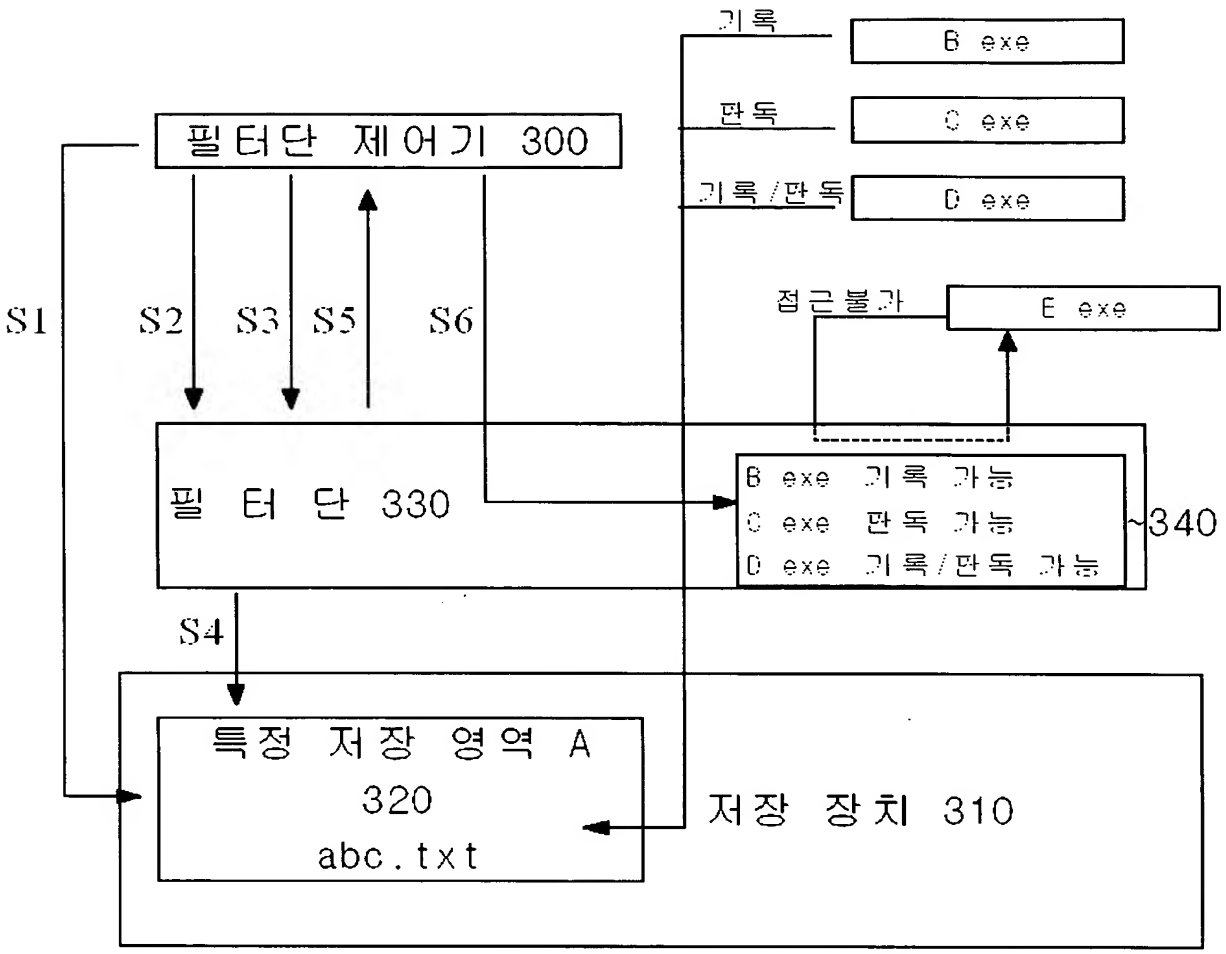
도면 1



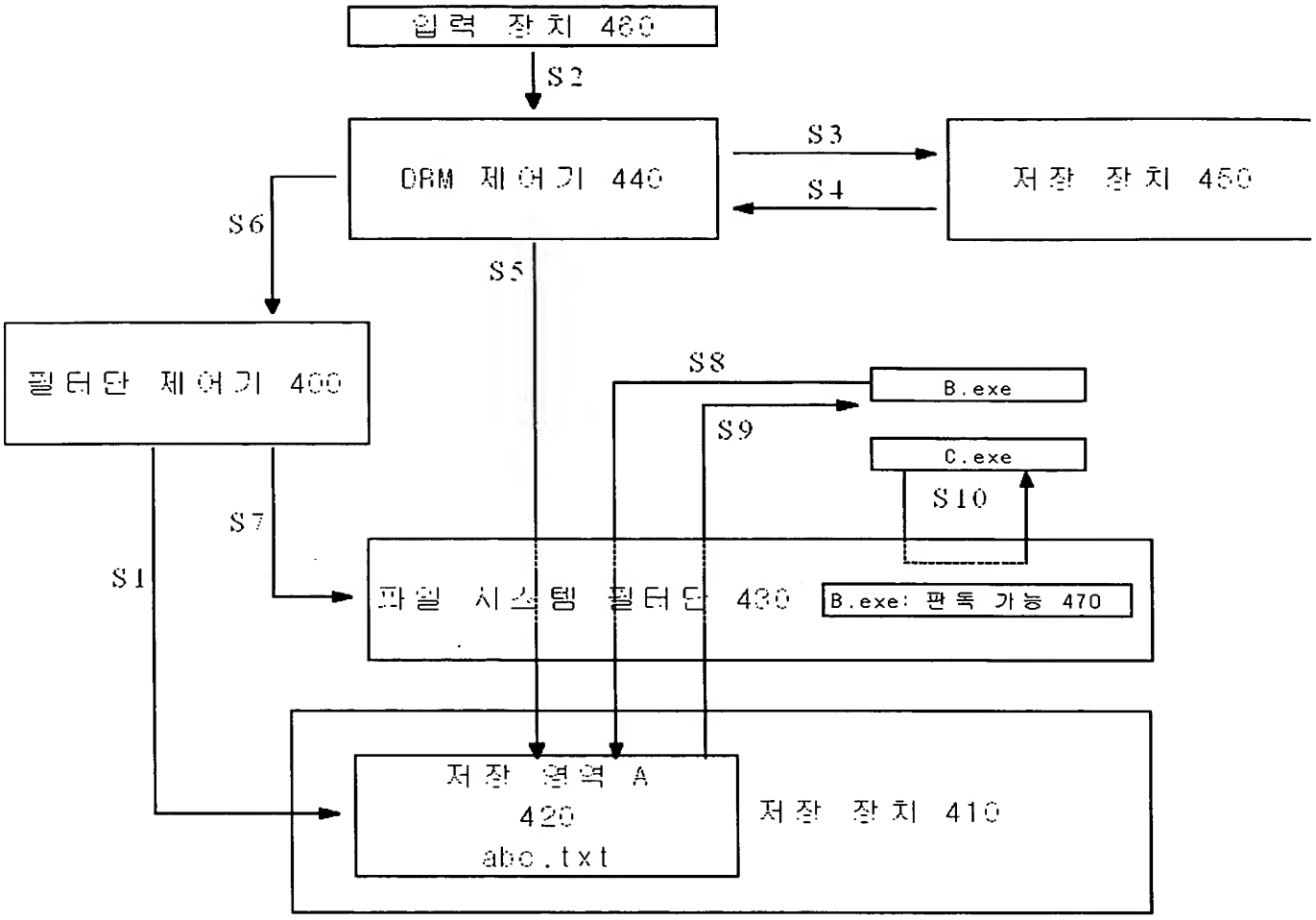
도면 2



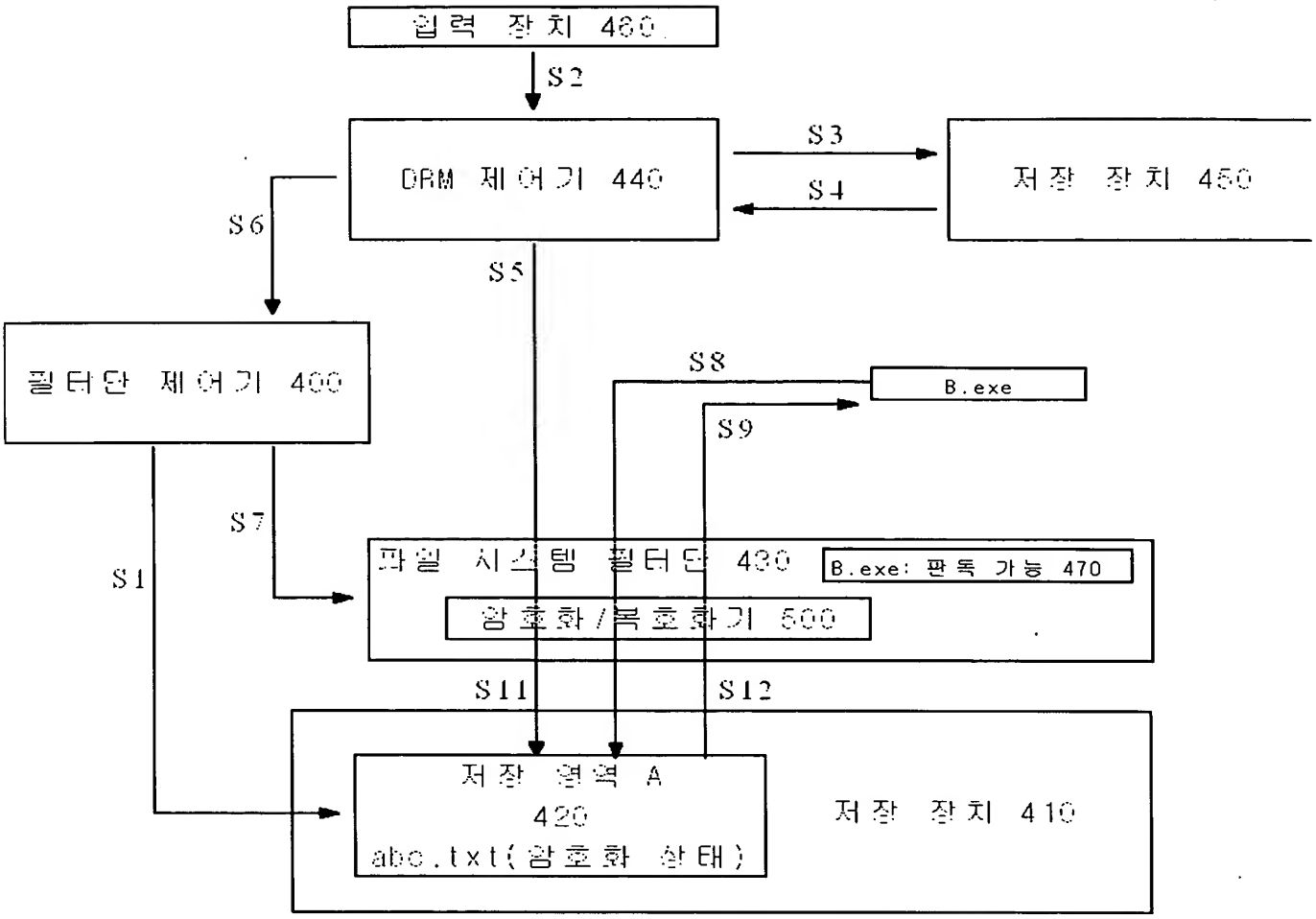
도면 3


기록
B exe
판독
C exe
기록/판독
D exe
필터단 제어기 300
접근불가
E exe
S1
S2
S3
S5
S6
필 터 단 330
B exe 기록 가능
C exe 판독 가능
D exe 기록/판독 가능
~340
S4
특정 저장 영역 A
320
abc.txt
저장 장치 310

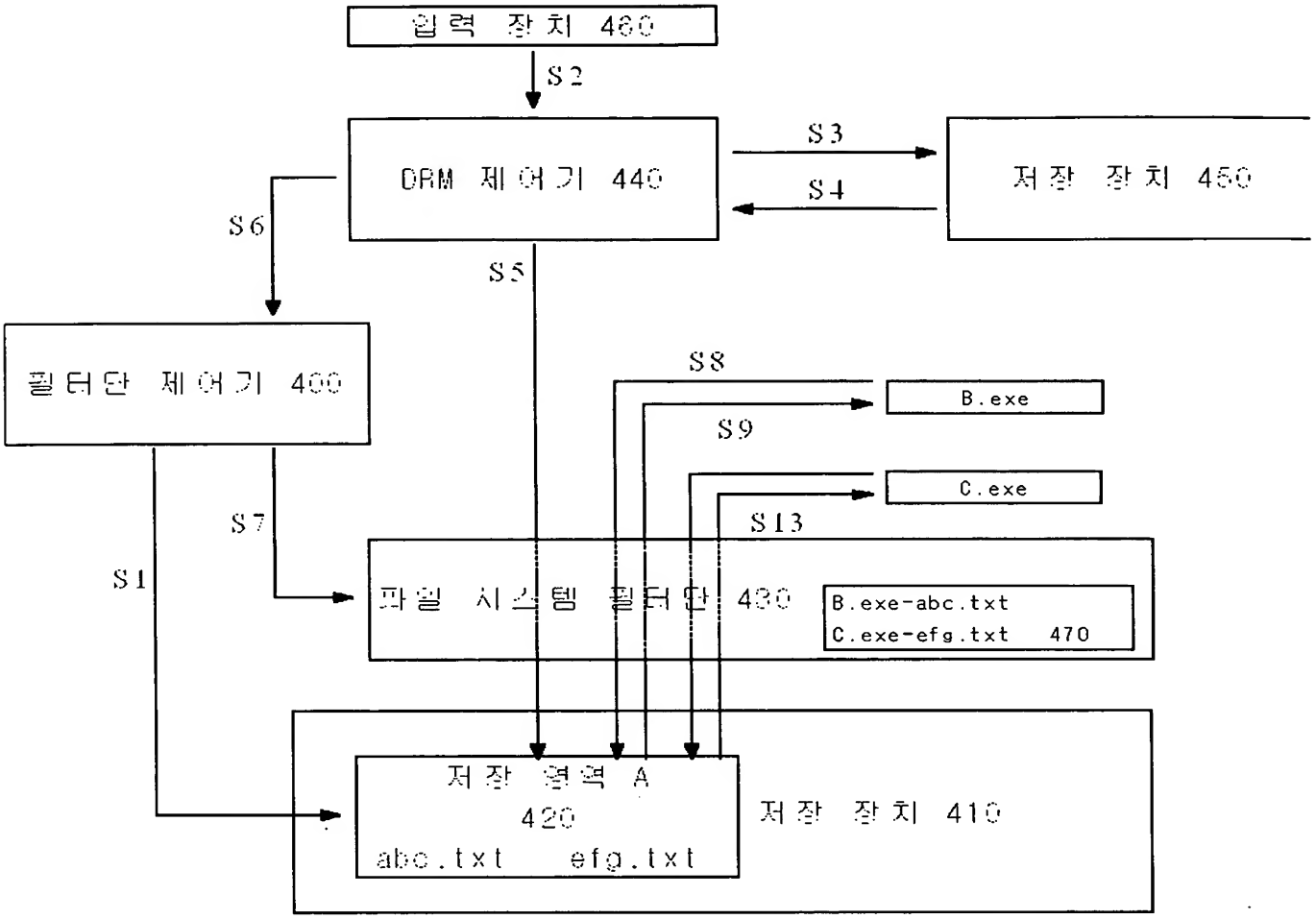
도면 4


입력 장치 460
S2
DRM 제어기 440
S3
S4
저장 장치 450
S6
S5
필터단 제어기 400
S8
B.exe
S9
C.exe
S10
S7
S1
파일 시스템 필터단 430
B.exe: 판독 가능 470
저장 영역 A
420
abc.txt
저장 장치 410

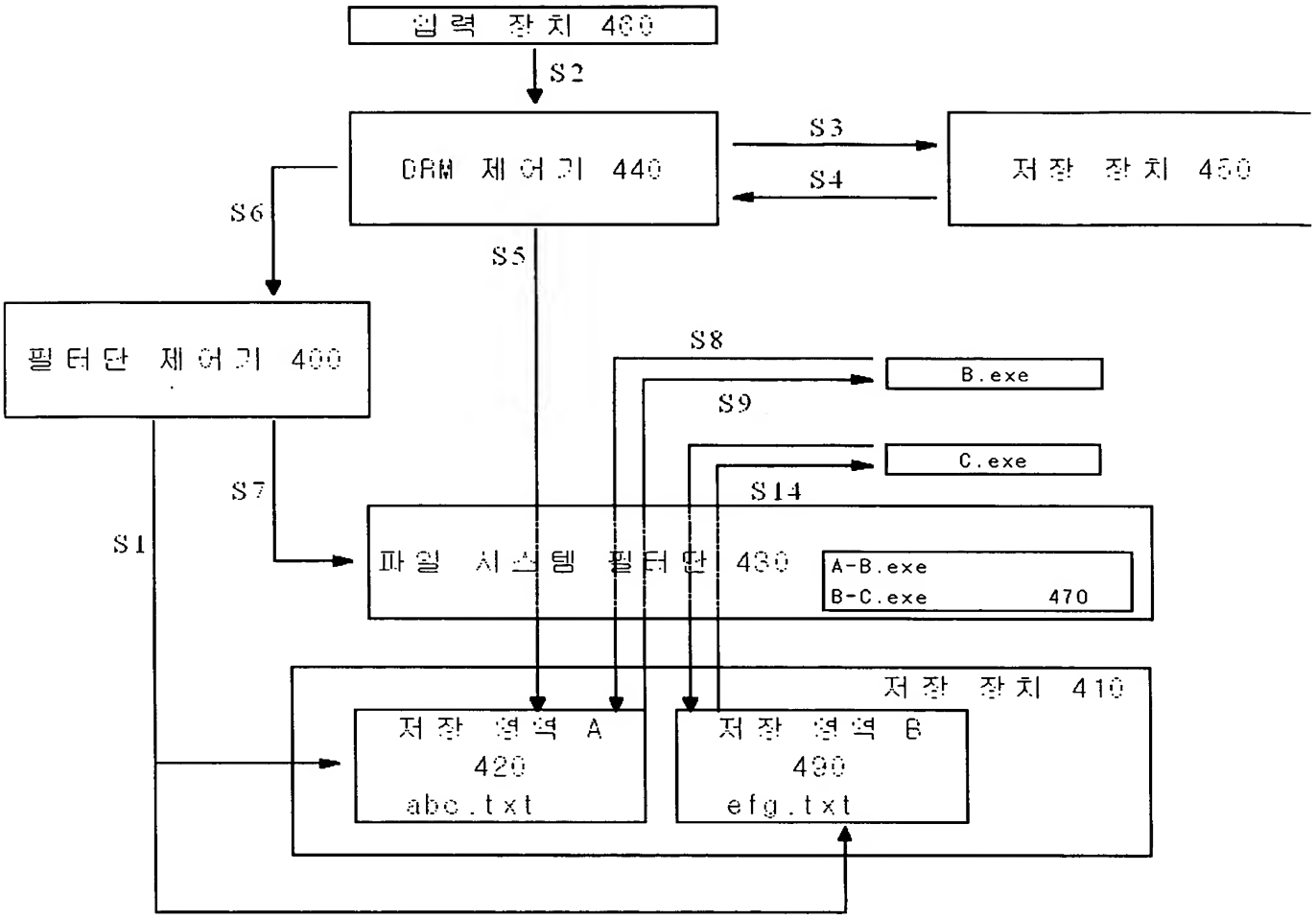
도면 5


입력 장치 460
S2
DRM 제어기 440
S3
S4
저장 장치 450
S6
S5
필터단 제어기 400
S8
B.exe
S9
S7
S1
파일 시스템 필터단 430
B.exe: 판독 가능 470
암호화/복호화기 500
S11
S12
저장 영역 A
420
abc.txt(암호화 상태)
저장 장치 410

도면 6


입력 장치 460
S2
DRM 제어기 440
S3
S4
저장 장치 450
S6
S5
필터단 제어기 400
S8
B.exe
S9
C.exe
S7
S13
S1
파일 시스템 필터단 430
B.exe-abc.txt
C.exe-efg.txt 470
저장 영역 A
420
abc.txt efg.txt
저장 장치 410

도면 7


입력 장치 460
S2
DRM 제어기 440
S3
S4
저장 장치 450
S6
S5
필터단 제어기 400
S8
B.exe
S9
C.exe
S14
S7
S1
파일 시스템 필터단 430
A-B.exe
B-C.exe
470
저장 장치 410
저장 영역 A
420
abc.txt
저장 영역 B
430
efg.txt